DEPARTMENT OF PERSONNEL & ADMINISTRATION	HIPAA Policy No.	8
	Current Effective Date	May 1, 2006
	Original Effective Date	May 1, 2006
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT	Approved by: Jeffrey C. Schutt Date: 4/26/06	
WORKSTATION USE AND SECURITY		

I. Purpose

To establish guidelines for managing workstations in ways that provide safety and security for electronic protected health information (ePHI).

II. Policy

It is the policy of the Department of Personnel and Administration (DPA) to protect ePHI by reasonably controlling workstation use and security. The following guidelines have been established to enforce this policy. These guidelines specify proper equipment operation procedures, functions to be performed, and the physical attributes of the surroundings of the workstation. Violations of this policy may result in corrective or disciplinary action in accordance with DPA's HIPAA Sanctions policy (see HIPAA Policy No. 5).

A. Set up and operation of a computer workstation must comply with the following guidelines:

1. Only computer systems, including desktops, laptops, peripherals, and other equipment (for example, PDAs) that meet DPA standards for such equipment and are owned and approved by DPA may be connected to DPA's network.

2. Only software or application programs authorized by DPA's Chief Information Officer (CIO) or delegate may be installed or loaded onto DPA's network and/or computer systems.

3. Only employees authorized to access ePHI may operate computer systems, applications, or software containing ePHI or through which ePHI can be accessed. Such employees must first be trained on how to use and how to shut down the system, application, or software.

4. Where appropriate, computer systems shall be secured to workstations in a manner prescribed by DPA's CIO or delegate. Except for laptops and other portable systems, employees must not move computer systems unless authorized to do so by DPA's CIO or delegate.

5. Computer screens must be positioned to avoid or minimize the likelihood of viewing of on-screen data by passersby.

6. Screensaver features must be turned on and set to activate after fifteen (15) minutes of inactivity to avoid or minimize the likelihood of viewing of on-screen data by passersby. Screensavers must be password-protected.

B. Employees performing authorized tasks involving use or disclosure of ePHI shall observe the following privacy and security practices:

- Do not share with or disclose to others your password or log-in code.
- Do not access a secure database in the presence of non-authorized persons.

- Do not leave your work area without first exiting any software application that contains ePHI.
- Be alert for any unusual incidents or unauthorized use or disclosure of ePHI and report such incident(s) to your supervisor.
- Do not copy or download ePHI data, except as authorized.
- Do not copy or download applications programs or software.
- Do not install other programs or software onto DPA computer systems unless authorized.
- Do not remove or delete programs, software, or system files unless authorized.

C. **Employees must comply with all other DPA policies regarding computer use.**

III. Procedures

Procedures regarding installation, movement, or removal or computer hardware, software, or downloadable applications shall be developed by DPA's CIO or delegate.

IV. Definitions/Abbreviations

None

V. Revision History

Date	Description
May 1, 2006	Original document

VI. References/Citations

HIPAA Security Rule

45 CFR Part 164.310(b)	Workstation Use
45 CFR Part 164.310(c)	Workstation Security